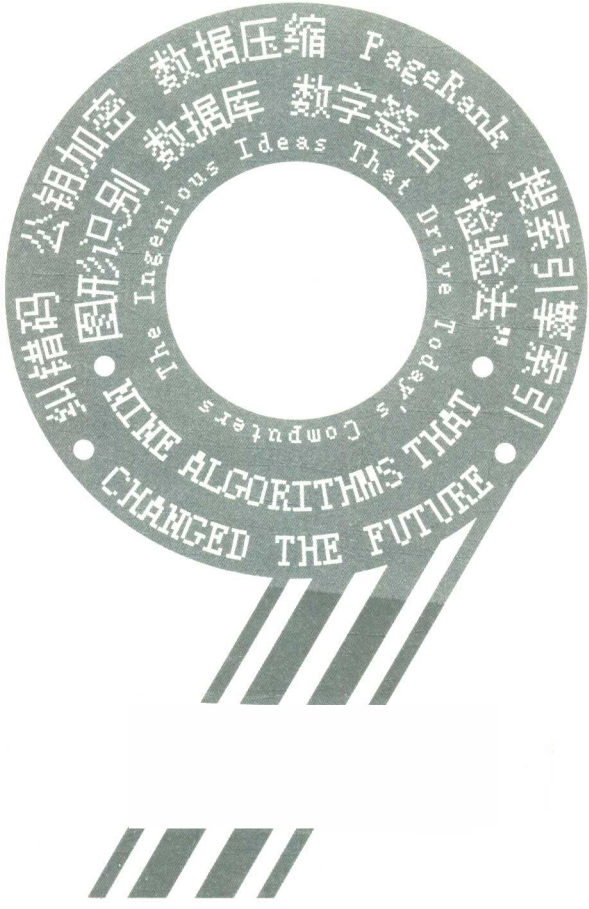
改变未来的九大算法



[美] 约翰·麦考密克（John MacCormick） 著
管策 译

改变未来的九大算法

[美] 约翰·麦考密克 著
（John MacCormick）

管策 译

NINE ALGORITHMS
THAT CHANGED THE FUTURE

The Ingenious Ideas That
Drive Today's Computers

中信出版集团 | 北京

图书在版编目（CIP）数据

改变未来的九大算法 /（美）约翰·麦考密克著；
管策译. -- 2 版. -- 北京：中信出版社，2019.2
书名原文：Nine Algorithms That Changed the
Future: The Ingenious Ideas That Drive Today's
Computers
ISBN 978-7-5086-9883-0

Ⅰ. ①改… Ⅱ. ①约… ②管… Ⅲ. ①计算机算法
Ⅳ. ①TP301.6

中国版本图书馆CIP数据核字（2018）第 287099

改变未来的九大算法

著　　者：[美] 约翰·麦考密克
译　　者：管策
出版发行：中信出版集团股份有限公司
（北京市朝阳区惠新东街甲 4 号富盛大厦 2 座　邮编　100029）
承 印 者：北京诚信伟业印刷有限公司

开　　本：880mm × 1230mm　1/32　　印　　张：9.25　　字　　数：213 千字
版　　次：2019 年 2 月第 2 版　　印　　次：2019 年 2 月第 1 次印刷
京权图字：01-2012-1063　　广告经营许可证：京朝工商广字第 8087 号
审 图 号：GS（2018）4060 号
书　　号：ISBN 978-7-5086-9883-0
定　　价：68.00 元

所获赞誉

荣获美国出版商协会“2012年计算机与信息科学最佳专业/学术图书奖”

作者解释了数亿人每天使用的一些算法，不是如算术和排序这类简单的算法，而是更复杂的事情——如何确定网页的重要性，以及无法被计算的问题。我强烈推荐这本书。

——查克•塞克（Chuck Thacker），
“图灵奖”得主

长久以来，没有哪本书能让我像十几岁时阅读霍金和费曼的书时那样让我兴奋，而这本书做到了，它提醒了我，为什么我喜欢计算机科学。

——安德鲁•菲茨吉本（Andrew Fitzgibbon），
“艾美奖”得主（相机软件开发者）

作者揭示了计算机科学家对算法着迷的原因：它们如此实用、美观和优雅。

——保罗•柯曾（Paul Curzon），
《科学》（*Science*）

一本关于关键算法的指南，阅读起来愉悦且轻松。它传达出一种奇妙的感觉——让电脑发挥魔力的是美丽的科学，而非技术。

——安德烈亚斯•特拉辛格（Andreas Trabesinger），
《自然物理学》（*Nature Physics*）

尽管人们对计算机充满兴趣，但并不了解其核心思想。这本书在向大众展示计算机科学这一艰巨的任务中取得了非凡的成就。

——欧内斯特•戴维斯（Ernest Davis），
SIAM News（美国工业和应用数学学会的新闻期刊）

大多数人对电子支付的安全性，或者电影如何被“塞进”光盘知之甚少，也不太关心，但作者认为它们富含惊人的独创性和创造力。

——罗伯特•马修斯（Robert Matthews），
《BBC聚焦》（*BBC Focus*，英国一本关于科学和技术的月刊）

作者用日常类比巧妙地解读核心算法，这对没有数学背景的读者来说很有用。想钻研算法的数学和计算机科学的学生也会感到受益颇深……这本书应该被图书馆珍藏。

——阿特•吉特尔曼（Art Gittleman），
就职于美国数学协会（MAA）

计算机专业人士和非专业人士都会对这本书感兴趣。作者并没有试图“用科学迷惑我们”，也没有“卖弄”其数学才能。相反，他采用了我们都能理解的简单类比。比如，作者用混合彩色颜料来类比公钥密码的原理，这非常精彩。

——克莱夫•马克斯菲尔德（Clive Maxfield），
《电子工程时报》（*EE Times*）

这本书适合对信息系统的工作原理感兴趣的人。

——约翰•吉尔比（John Gilbey），
就职于泰晤士高等教育出版社（Times Higher Education）

序

计算机行业正在改变我们的社会，正如物理学和化学在前两个世纪给社会带来的巨大改变一样。的确，数字技术几乎影响甚至颠覆了我们生活的方方面面。鉴于计算机行业对现代社会的重要性，人们对让这一切成为可能的基本概念却知之甚少，这显得有点儿自相矛盾。对这些概念的研究是计算机科学的核心，而麦考密克的这本新书则是向大众展示这些概念的少数书籍之一。

人们较少视计算机科学为一门学科，其中一个原因是，高中极少开设计算机科学这门课程。虽然人们通常认为要强制开设物理学和化学这两门基础课程，但作为独立学科的计算机科学，却通常只在大学阶段才被开设。况且，学校讲授的“计算机”或“信息与通信技术”知识，通常只是略高于使用软件的技能训练。因此，学生们认为计算机学科枯燥也并不意外；而他们在娱乐和通信上使用计算机技术的天然热情，也因为实现这类技术的学术深度而有所消退。这些问题被认为是导致过去 10 年大学计算机科学专业学生人数下降一半的主要原因。考虑到数字技术对现代社会的极度重要性，让人们重新领略计算机科学的奇妙之处已经刻不容缓。

2008 年，我很荣幸地被选为第 180 届英国皇家科学院圣诞讲座（Royal Institution Christmas Lectures）的演讲人，该讲座由迈克尔·法拉第（Michael Faraday）于 1826 年发起。2008 年圣诞讲座的主题首次涉及计算机科学。在准备这些讲座时，我花了很多时间来思考如何向大众解释计算机科学，却发现能提供解决这一需求问题的资源很少，几乎没有关于计算机科学的畅销书。因此，我特别高兴能看到麦考密克的这本书。

麦考密克在面向大众介绍计算机科学的复杂思想方面做得非常好。这其中的许多思想极其新颖，仅从这点上来看，它们就很值得关注。举个例子：电子商务的爆炸式增长之所以成为可能，是因为它具备了能在互联网上秘密、安全地发送机密信息（如信用卡卡号）的能力。数十年来，建立在“开放”通道上的保密通信被认为是一个科学难题。当人们发现解决方法时，他们才发觉保密通信是精美的艺术。而麦考密克也以精确的类比进行了解释，读者无须拥有计算机科学知识就能理解。这些优点使这本书在科普读物领域做出了不可估量的贡献，我极力推荐这本书。

克里斯·毕晓普（Chris Bishop）
微软剑桥研究院资深科学家
大不列颠皇家学院副院长
爱丁堡大学计算机科学教授

前 言

计算机日常运用的卓越思想

计算机科学中的伟大思想是如何诞生的？以下遴选部分思想进行介绍：

- 20 世纪 30 年代，在第一台数字计算机被发明以前，一位英国天才开创了计算机科学研究领域。之后，这位天才还继续证明了，不管未来建造的计算机运行多快、功能多强大、设计得多好，仍旧有一些问题将是计算机不能解决的。
- 1948 年，一位供职于电话公司的科学家发表了一篇论文，由此开创了信息理论研究领域。这位科学家的工作让计算机能以完美的精确度传输信息，即便大部分数据都因为被干扰而遭受破坏。
- 1956 年，一群学者在达特茅斯（Dartmouth）举行会议。这次会议的目标很清晰，也很大胆，那就是开创人工智能领域的研究。在取得了许多重大成功，也经历了无数次失望之后，我们仍期待出现一个真正的智能计算机程序。
- 1969 年，IBM（国际商业机器公司）的一名研究人员发明了一种在数据库中组织信息的先进方法。目前，绝大多数在线交易都使

用该技术存储及检索信息。

- 1974 年，英国政府秘密通信实验室的研究人员发明了一种让计算机实现安全通信的方法，即另一台计算机可以查看在计算机之间交换的所有信息。这些研究人员为政府保密所限——不过幸运的是，三名美国专家独立开发并拓展了这项重大发明，为互联网上所有的安全通信打下了基础。
- 1996 年，斯坦福大学的两名博士生决定联手搭建一个互联网搜索引擎。几年后，他们创办了谷歌公司——互联网时代的第一个数字“巨头”。

我们在享受 21 世纪技术惊人增长的同时，使用计算机设备——不管是现有最强大的一组机器，还是最新、最时尚的手持设备——不可避免地要依赖计算机科学的基础思想，而这些思想都诞生于 20 世纪。想一想：你今天做过什么令人印象深刻的事情吗？好吧，这个问题的答案取决于你怎么看。也许是你搜索了包含数十亿份文档的资料库，从中选出两三份与你的需求最相关的文档？即便有能够影响所有电子设备的电磁干扰，你在存储或传输数百万条信息的过程中，也没犯一点儿错误？你是否成功地完成了一次在线交易，即便同时有成千上万名消费者在访问同一个服务器？你是否在能够被其他数十台计算机嗅探到的线路中传输了一些机密信息（比如信用卡卡号）？你是否运用过压缩的魔力，将数兆的照片压缩成更易于管理的大小，以便附在电子邮件中发送？你是否在手持设备上触发了人工智能，以自动纠正你在手持设备的小巧键盘上输入的内容？

这些令人印象深刻的壮举都有赖于之前提到的伟大发明或发现。然而，绝大多数计算机用户每天都会多次运用这些天才的想法，却从没有意识到！本书旨在向大众解释这些观点——我们每天使用的计算机科学的伟大思想。在解释每一个观点时，我都假设读者不了解有关计算机科学的任何知识。

算法：指尖“精灵”的构件

到目前为止，我一直在谈计算机科学的伟大“思想”，但计算机科学家们会将许多重要思想形容为“算法”。那么思想和算法之间有什么区别？究竟什么是算法？这一问题最简单的答案是，算法是一张精确的处方，它按顺序详细列出了解决一个问题所需要的具体步骤。我们小时候在学校学到的一种算法就是很好的例子：将两个大数字相加的算法。如下例所示。这个算法涉及一连串的步骤，开始的步骤如下：“首先，将两个数的最末位数相加，写下结果的最末位数，将剩下的数放到左侧的下一栏；接着，将下一栏的数相加，再将除了结果末位数的数字和前一栏余下的数相加……”依此类推。

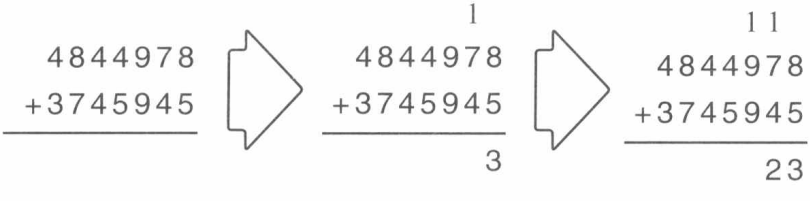


图 1　将两个数字相加的算法的前两步

请注意算法步骤近乎机械化的感觉。事实上，这是算法的关键特

点之一：每步都必须绝对精确，没有任何人类意图或推测掺杂其中。这样，每个完全机械化的步骤才能被编入计算机。算法的另一个重要特点是，不管输入什么，算法总能运行。我们在学校学到的相加算法就拥有这一特性：不管你想把哪两个数相加，运用算法最终都会得出正确答案。比如，用这一算法将两个长达 1 000 位的数相加，你肯定能得到答案，尽管这需要相当长的时间。

对把算法定义为一张精确的机械化的处方的说法，你也许会略感好奇。这张处方究竟要多精确？要进行哪些基本操作？比如，在上面的相加算法中，简单地说一句“把两个数相加”是不是就行了？还是说我们要在加法表上列出所有位的数字？这些细节看起来也许有点儿乏味，甚至会显得有点儿学究气，但它们其实离真相不远了：这些问题的真正答案正处于计算机科学的核心，并且也和哲学、物理学、神经科学及遗传学有联系。有关算法究竟是什么的深层问题都归结于一个前提——众所周知的邱奇-图灵论题（Church-Turing thesis）。我们将在第九章重温这些问题，届时我们还将讨论计算的理论极限，以及邱奇-图灵论题的一些方面。同时，将算法比作一张非常精确的处方这一非正式观点，其效果会非常好。

现在我们知道了什么是算法，但算法和计算机有什么联系呢？关键在于，计算机需要用非常精确的指令编程。因此，在能让计算机为我们解决某个特定问题之前，我们需要为那个问题开发一种算法。在数学和物理学等其他学科中，重要的结果通常是由一个方程式获得的。（著名的例子包括勾股定理 $a^2+b^2=c^2$ 或爱因斯坦的质量守恒定理 $E = mc^2$。）相反，计算机科学的伟大思想通常是来形容如何解决一个

问题的——当然，是使用一种算法。因此，本书的主要目的是，解释让计算机成为你的个人天赋的东西——计算机每天使用的伟大算法。

一种伟大的算法由什么构成?

这会引出一个刁钻的问题：什么才是真正伟大的“算法”？潜在的候选算法清单相当长，但我用几条基本标准缩减了用于本书的候选算法清单。第一条也是最重要的一条标准是，伟大的算法要被普通计算机用户每天用到。第二条重要的标准是，伟大的算法应该能处理具体的现实问题，如压缩一个特定文件或通过一个噪链精确地传输文件。对已经了解部分计算机科学的读者而言，第XIII页文字框中的内容将解释前面两大标准的部分后果。

第三个标准是，算法主要和计算机科学理论相关。这排除了主要和计算机硬件——如CPU（中央处理器）、监视器，以及网络——有关的技术。这条标准也减轻了对基础设施——如互联网——设计的重视。为什么我要着重于计算机科学理论？部分原因是公众对计算机科学认知的不平衡：有一种广泛的观点认为，计算机科学基本上就是编程（如“软件”）和设备设计（如“硬件”）。事实上，最美妙的计算机科学思想中有许多是十分抽象的，并不属于以上任意一类。我希望通过强调这些理论思想，让更多人将计算机科学作为一门知识学科来理解。

你也许已经注意到了，我列出的标准可能会遗漏一些伟大的算法，但我从一开始就避免了定义“伟大”这个极其麻烦的问题。针对

这一问题，我依赖于自己的直觉。在本书说明的每种算法中，其核心都是一个让整件事情奏效的精巧把戏（trick）。对我而言，当这个把戏显露出来时，那个“啊哈时刻”（即“aha”moment，指用户体验产品时眼前一亮的那一刻）会让解释这些算法成为令人愉悦的经历，我希望你也能有此感受。我会用到“把戏”这个词很多次，需要指出的是，我并非指那些卑劣或骗人的把戏——孩子可能会用在弟弟或妹妹身上的那种把戏。相反，本书中的把戏类似于交易诀窍或魔术：为达成目标而采用的聪明技巧，否则目标很难达成或根本不可能达成。

因此，根据直觉，我选出了自认为是计算机科学世界中最精巧、最神奇的把戏。在英国数学家高德菲·哈罗德·哈代（G. H. Hardy）的《一个数学家的辩白》（*A Mathematician's Apology*）中，作者试图向公众解释数学家从事数学的原因——“美是第一道测试：丑陋的数学在这个世界中无永存之地”。这道“美的测试”也适用于在计算机科学中蕴含的理论思想。因此，选取在本书中出现的算法的最后一条标准，就是哈代的——也许可以这么称呼——“美的测试”：我希望至少能成功地向读者展示部分美——我在每种算法中感受到的美。

第一条标准——要被普通计算机用户每天用到——排除了主要由计算机专业人士使用的算法，如编译器和程序验证技术。第二条标准——解决某个特定问题的具体程序——排除了许多作为计算机科学本科课程核心内容的伟大算法，如排序算法（快速排序等）、图形算法（迪杰斯特拉最短路径算法等）、数据结构（哈希表等）。这些算法的伟大性毋庸置疑，而且很轻易地就满足了第一

> 条标准，因为普通用户使用的绝大多数应用程序都会反复应用这些算法。但这些算法太通用了：它们能被用来解决众多问题。在本书中，我决定要专注于解决特定问题的算法，因为对普通计算机用户而言，这些算法能让他们拥有更清晰的动机。

接下来我将谈谈选择展示的这些算法。搜索引擎的巨大影响，也许是算法技术影响所有计算机用户最明显的例子，我自然也将部分互联网搜索的核心算法收在了本书中。第一章描述了搜索引擎如何使用索引寻找与请求匹配的文件，而第二章则解释了网页排名（PageRank）算法——谷歌公司为保证匹配度最高的文件出现在搜索结果列表顶部的原始算法。

即便我们不经常想这件事情，绝大多数人也能意识得到，为提供出人意料的强大搜索结果，搜索引擎会落实一些深邃的计算机科学思想。相反，其他一些伟大的算法也经常被用到，但计算机用户对此甚至都没有意识到。第三章描述的公钥加密（Public Key Cryptography）就是这样一种算法。用户每次访问一个安全网站（地址以https而非http开头），都会用到公钥加密的一个方面——众所周知的密钥交换（key exchange）——来展开一段安全对话。第三章就是在解释密钥交换过程的实现原理。

第四章的主题是纠错码（Error Correcting Codes），这是我们经常使用但没有意识到的另一类算法。事实上，纠错码极有可能是有史以来唯一一种使用次数最频繁的伟大算法。纠错码可以让计算机识别并纠正在储存或传输数据时出现的错误，而不必依靠备份或再次传输。

纠错码无处不在：它们被用于所有硬盘驱动器、众多网络传输、CD（数字光盘）和DVD（高密度数字视频光盘），甚至还存在于一些计算机的内存中。不过，纠错码的能力太强了，以至于我们意识不到它们的存在。

第五章稍微有点儿特殊，它介绍的是图形识别算法（Pattern Recognition Algorithm）。图形识别算法也能进入伟大的计算机科学思想榜单，但它违背了第一条标准：要被普通计算机用户每天用到。图形识别属于计算机识别高度可变信息——如笔迹、讲话和人脸——的技术。事实上，在21世纪的第一个十年里，绝大多数日常计算并没有用到这些技术。但在2010年，图形识别的重要性急剧增大：配备小型屏幕键盘的移动设备需要自动纠错，平板设备必须识别手写输入，而且所有这些设备（特别是智能手机）越来越趋向于语音操作。一些网站甚至使用图形识别来决定向用户展示哪种广告。另外，我对图形识别也有偏好，因为它是我的研究领域。因此，第五章描述了三种最有趣、最成功的图形识别技术：最近邻分类器（Nearest-neighbor Classifier）、“决策树”（Decision Tree），以及神经网络（Neural Network）。

第六章讨论了压缩算法。压缩算法组成了另一组使计算机变成我们“指尖精灵”的伟大思想。计算机用户的确会时不时地直接进行压缩，也许是为了节省磁盘空间，也许是为了缩减照片容量，以便用电子邮件发出。不过在私底下，压缩使用的频率要更高：我们根本没有意识到，我们的下载或上传也可以通过压缩以节省带宽，而数据中心通常会压缩消费者的数据以降低成本。电子邮件提供商提供给你的5

GB（计算机存储单位）空间，经压缩后很有可能只占据电子邮件提供商 5 GB空间的很小一部分。

第七章讲到了数据库中运用的一些基础算法。这一章侧重为实现一致性——指一个数据库中的关系不互相冲突——而采用的聪明技巧。没有这些精巧的技术，我们的绝大部分在线生活［包括网络购物以及通过Facebook（“脸书”）之类的社交网站进行互动］就会消亡于众多计算机错误中。这一章解释了一致性真正的问题是什么，以及计算机科学家是如何解决这一问题的。前提是不牺牲我们所期望的在线系统拥有的高效性。

在第八章，我们会了解理论计算机科学无可争议的瑰宝之一：数字签名。乍看之下，用数字形式“签署”一份电子文档似乎不可能。你也许会想，这种签名必须由数字信息组成，而任何想要伪造签名的人都可以毫不费力地拷贝这些信息。这一悖论的解决方案，就是计算机科学取得的最令人瞩目的成就之一。

第九章采取了截然不同的视角：与其描述一种已经存在的伟大算法，我们不如去了解一种假如存在则必然会伟大的算法。不过我们会震惊地发现，这种特别伟大的算法不可能存在。这表明计算机解决问题的能力存在绝对极限，而我们将简单地从哲学和生物学角度探讨这一结果的应用。

在结语部分，我们会总结伟大算法的一些共性，花些时间畅想未来会怎样。会有更多伟大算法出现吗？或者说，我们已经发现了所有伟大的算法？

在此，不得不提前说一下本书的风格。任何科普作品都必须清楚

地告知读者信息来源，但引用会破坏文本的流畅性，并让读者产生阅读学术著作的感觉。由于可读性和易读性是本书的首要目标，所以本书正文不会出现引用。不过，我清楚地记录了所有来源，并在本书末尾的“注释”板块中列出，还时不时地附上拓展评论。这个板块还列出了一些额外材料，以便感兴趣的读者能去寻找更多和计算机科学中伟大算法有关的信息。

为什么我们要关注这些伟大的算法?

希望对这些迷人思想的快速总结能让你渴望深入了解它们的运行方式。不过，也许你仍然在思考：本书的终极目标是什么？让我简短地介绍一下本书的真正目的。这本书绝不是一本问答式操作手册。在读完本书后，你不会成为计算机安全方面的专家，也不会成为人工智能或其他领域的专家。你也许能学到一些有用的技能，这倒是真的。比如：你会对如何检查“安全”网站凭证以及“已签名”软件包了解更多；你能在有损和无损压缩之间针对不同任务做出明智选择；通过理解搜索引擎索引和排名技术的某些方面，你能更高效地使用搜索引擎。

然而，这些相对于本书真正的目的不过是微小的红利。在读完本书后，你不会成为一名更加熟练的计算机用户，但你会更加珍视每天在所有计算设备上不停使用的思想的美。

为什么这是件好事？我用类比的方式来说明。我肯定不是一位天文学专家——事实上，我在这个领域里相当无知，我想知道更多。但